

✓ ○ 1) On munit l'ensemble $A = \mathbb{Z} \times \mathbb{Z}$ des deux lois internes

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{et} \quad (a, b) \cdot (a', b') = (aa', 0)$$

✗ Montrer que $(A, +, \cdot)$ est un anneau commutatif. ^{non unitaire} Quels sont les diviseurs de 0 dans A ?

✓ ○ 2) On note cette fois-ci $E = \mathbb{Z} \times \mathbb{Z}$ et l'on définit les opérations internes

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{et} \quad (a, b) \cdot (a', b') = (aa' - bb', ab' + ba')$$

Montrer que $(E, +, \cdot)$ est un anneau commutatif unitaire. Est-il intègre ? Déterminer les diviseurs de l'unité dans E .

3) L'anneau des entiers de Gauss est $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} / a, b \in \mathbb{Z}\}$. Vérifier que $\mathbb{Z}[i]$ est un sous-anneau de \mathbb{C} et qu'il est isomorphe à B .

Solution :

Exercice : a) On note $A = \mathbb{Z} \times \mathbb{Z}$. On munit A des 2 lois

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{et} \quad (a, b) \cdot (a', b') = (aa', 0)$$

Montrer que A est un anneau commutatif et trouver tous les diviseurs de 0.

b) On pose cette fois-ci :

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{et} \quad (a, b) \cdot (a', b') = (aa' - bb', ab' + ba')$$

Montrer que A est un anneau commutatif unitaire. Est-il intègre ?

Déterminer les diviseurs de l'unité.

~~tous les él. de A diviseurs sont des div. de 0. En effet : $\forall (a, b) \in A$~~

Sol. : a) $aa' = 0$ donc ~~les diviseurs de 0 de A sont $(0, 0)$ et $(a, b)(0, 1) = (0, 0)$~~

b) Notons $1 = (a', b')$ l'unité de A . On aura :

$$\begin{cases} aa' - bb' = a \\ ab' + ba' = b \end{cases} \quad \forall a, b \Rightarrow \begin{cases} a' = 1 \\ b' = 0 \end{cases} \quad \text{Donc } \boxed{1 = (1, 0)}$$

* A intègre ?

$$(1) \begin{cases} aa' - bb' = 0 \\ ab' + ba' = 0 \end{cases} \Rightarrow abb' + b^2a' = 0 \quad \text{donc} \quad \begin{aligned} a^2a' + b^2a' &= 0 \\ a'(a^2 + b^2) &= 0 \end{aligned}$$

d'où $a' = 0$ si $(a, b) \neq (0, 0)$.

$$\text{Mais alors, (1) donne : } \begin{cases} bb' = 0 \\ ab' = 0 \end{cases} \Rightarrow b' = 0.$$

Ainsi, si $(a, b) \cdot (a', b') = 0$ et $(a, b) \neq (0, 0)$ on a : $(a', b') = (0, 0)$ ie A intègre.

* Diviseurs de 1 ?

$$\begin{cases} aa' - bb' = 1 & (2) \\ ab' + ba' = 0 & (3) \end{cases}$$

$$\text{Si } a \neq 0, \quad b' = -\frac{a'}{a}b \quad \text{donc} \quad aa' + b\frac{a'}{a}b = 1 \Rightarrow \begin{cases} a' = \frac{a}{a^2 + b^2} \\ b' = -\frac{b}{a^2 + b^2} \end{cases}$$

Comme $a' \in \mathbb{Z}$, cela entraîne $\begin{cases} a = \pm 1 \\ b = 0 \end{cases}$, mais alors (3) donne $\begin{cases} a' = \pm 1 \\ b' = 0 \end{cases} \leftarrow \text{ordre à respecter}$

$$\text{Ainsi } \boxed{(\pm 1, 0) \cdot (\pm 1, 0) = 1}$$

$$\text{Si } a = 0, \quad (2) \text{ et } (3) \text{ s'écrivent : } \begin{cases} bb' = -1 \\ ab' + ba' = 0 \end{cases} \quad \text{ie } \begin{cases} (0, 1)(0, -1) = 1 \\ \text{ou} \\ (0, -1)(0, 1) = 1 \end{cases}$$

Conclusion : Les diviseurs de 1 sont de la forme $(0, \pm 1)$ ou $(\pm 1, 0)$.

Soit a un élément d'un anneau principal A . Montrer que :

1) a est irréductible si, et seulement si, a est premier avec tout nombre qu'il ne divise pas.

2) a est irréductible si, et seulement si, il vérifie l'assertion suivante :

$$a|bc \Rightarrow a|b \text{ ou } a|c$$

Solution :

Soit A un anneau principal.

Hq:

- a) a irréductible $\Leftrightarrow a$ est premier avec tout nbre qu'il ne divise pas
 b) a irréductible $\Leftrightarrow \{ a \mid pq \Rightarrow a \mid p \text{ ou } a \mid q \}$
-

a) (\Rightarrow) Si $a \nmid b$ et si d est un diviseur commun à a et b , $d \mid a$ donc $d = au$ ou u (avec $u \in A^*$).

$d = au$ est impossible (sinon $a \mid d \mid b$) donc $d = u \in A^*$

On a montré: $d \mid a$ et $d \mid b \Leftrightarrow d \in A^*$

ie $a \wedge b = 1$

(\Leftarrow) Soit $a = pq$.

Si $a \mid p$, $p = aa'$ et $a = aa'q \Rightarrow 1 = a'q \Rightarrow q \in A^*$

Si $a \nmid p$, $a \wedge p = 1$ et le th. de Gauss entraîne $a \mid q$. On montre alors que $p \in A^*$ comme ci-dessus.

b) (\Rightarrow) Si a irréductible, soit $a \mid pq$. a est premier avec tout él. qu'il ne divise pas, donc:

si $a \nmid p$ alors $a \wedge p = 1$ et le th. de Gauss entraîne $a \mid q$

(\Leftarrow) Si $a = pq$, alors $a \mid pq$ donc $a \mid p$ ou $a \mid q$

Supposons $a \mid p$. On aura $p = au$ et $a = auq \Rightarrow 1 = uq \Rightarrow \begin{cases} u \in A^* \\ q \in A^* \end{cases}$
 donc p est irréductible.

Anneaux de fractions $S^{-1}A$.

Soit A un anneau commutatif et unitaire, mais non nécessairement intègre. Une partie S de A est dite multiplicative si elle vérifie

$$1 \in S, 0 \notin S \text{ et } \forall x \in S \quad \forall y \in S \quad xy \in S.$$

1) Soit \mathcal{R} la relation dans l'ensemble $A \times S$ définie par

$$\forall (a, s), (a', s') \in A \times S \quad (a, s) \mathcal{R} (a', s') \Leftrightarrow \exists t \in S \quad (as' - sa')t = 0.$$

Montrer que \mathcal{R} est une relation d'équivalence. On notera $\frac{a}{s}$ la classe d'équivalence du couple (a, s) , et $S^{-1}A$ l'ensemble quotient $A \times S / \mathcal{R}$. Vérifier que les lois

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + sa'}{ss'} \text{ et } \frac{a}{s} \times \frac{a'}{s'} = \frac{aa'}{ss'}$$

définissent sur une structure d'anneau. Vérifier que l'application $i : A \rightarrow S^{-1}A$ définie par $i(a) = \frac{a}{1}$ est un morphisme d'anneaux. Est-il injectif ?

2) A partir de cette question et jusqu'à la fin du problème, on suppose que l'anneau A est intègre. Quelle simplification cela entraîne-t-il dans la définition de \mathcal{R} ? Que devient l'application i ? Peut-on considérer A comme un sous-anneau de $S^{-1}A$?

3) Si R est un anneau, on note \mathcal{P}'_A l'ensemble des idéaux premiers de A n'interceptant pas S , et $\mathcal{P}_{S^{-1}A}$ l'ensemble des idéaux premiers de $S^{-1}A$. Montrer que l'application

$$\begin{aligned} \Phi : \mathcal{P}'_A &\rightarrow \mathcal{P}_{S^{-1}A} \\ I &\mapsto S^{-1}I = \left\{ \frac{i}{s} / i \in I \text{ et } s \in S \right\} \end{aligned}$$

est bijective croissante d'inverse $J \mapsto J \cap A$.

4) **Anneau local.** De façon générale et si A est un anneau intègre, montrer l'équivalence entre les propriétés :

- i) A ne possède qu'un seul idéal maximal,
- ii) l'ensemble $A \setminus A^*$ des éléments non inversibles de A forme un idéal.

Lorsque l'une des propriétés ci-dessus est vérifiée, on dit que A est un anneau local, et l'on remarque qu'alors l'unique idéal maximal \mathcal{M} de A est $\mathcal{M} = A \setminus A^*$.

5) Soit t un élément non nul d'un anneau intègre A et $S_t = \{1, t, t^2, \dots\}$.

a) Montrer que S_t est une partie multiplicative de A . On pose

$$A_t = S_t^{-1}A = \left\{ \frac{a}{t^n} \in \text{Frac}(A) / a \in A \text{ et } n \in \mathbb{N} \right\}$$

où $\text{Frac}(A)$ désigne le corps des fractions de A .

b) Supposons maintenant que $A = \mathbb{Z}$ et que t soit un nombre entier premier. Expliciter le groupe multiplicatif \mathbb{Z}_t^* et montrer que l'anneau \mathbb{Z}_t est local. Quels sont les idéaux premiers de \mathbb{Z}_5 ?

c) Décrire les idéaux premiers de \mathbb{Z}_{42} .

6) Soit t un élément non nul de l'anneau intègre A .

a) Montrer qu'il y a correspondance bijective entre les idéaux premiers de A_t et les idéaux premiers de A ne contenant pas t .

b) Montrer qu'il y a correspondance bijective entre les idéaux premiers de $A/(t)$ et les idéaux premiers de A contenant t .

c) Quels sont les idéaux premiers de $\mathbb{Z}/42\mathbb{Z}$?

7) Soit I un idéal premier d'un anneau intègre A .

a) Montrer que la partie $S_I = A \setminus I$ est multiplicative. On pose $A_I = S_I^{-1}A$.

b) Montrer que l'anneau A_I est local.

c) Quels sont les idéaux premiers de $\mathbb{Z}_{(5)}$? de $\mathbb{Z}/5\mathbb{Z}$?

⁰[uann0019] Dany-Jack Mercier (réf. Milne p12 par exemple)

1) Il est facile de voir que R est Reflexive et Symétrique.
Montrons la transitivité. Il faut prouver que

$$\left. \begin{array}{l} (a, s) R (a', s') \\ (a', s') R (a'', s'') \end{array} \right\} \Rightarrow (a, s) R (a'', s'')$$

Supposons donc qu'il existe $t, u \in S$ tq

$$\begin{cases} (as' - sa')t = 0 \\ (a's'' - s'a'')u = 0 \end{cases}$$

Cela entraîne

$$\begin{cases} (as''s' - ss'a')tu = 0 \\ (a'ss'' - s'sa'')ut = 0 \end{cases}$$

$$(as'' - sa'')s'ut = 0$$

et prouve bien que $(a, s) R (a'', s'')$.

(---)

$$\frac{a}{s} \cdot \frac{b}{s'} \in S^{-1}I \Leftrightarrow \frac{ab}{ss'} = \frac{c}{s''} \quad c \in I$$

$$\Rightarrow abs'' = ss'c \in I \Rightarrow a \in I \text{ ou } b \in I \quad (\text{puisque } \text{hyp} \Rightarrow s'' \notin I)$$

2) (---)

3) Φ est bien définie car $S^{-1}I$ est un idéal premier de $S^{-1}A$ dès que I est un idéal premier de A .
On suppose ici que $A \subset S^{-1}A$ via le monomorphisme $i: A \rightarrow S^{-1}A$.
Si J est un idéal de $S^{-1}A$, alors $J \cap A$ sera un idéal de A .
Il reste à montrer que :

$$\begin{cases} (1) & S^{-1}I \cap A = I & \forall I \in \mathcal{P}'_A \\ (2) & S^{-1}(J \cap A) = J & \forall J \in \mathcal{P}_{S^{-1}A} \end{cases}$$

Preuve de (1) : $S^{-1}I \cap A \supset I$ est trivial. Réc., si $x \in S^{-1}I \cap A$, alors $x = \frac{c}{s} = a \in A$ où $c \in I$ et $s \in S$. Donc $c = as \in I \Rightarrow a \in I$ ou $s \in I$ (puisque I est premier). Comme par hypothèse $s \notin I$, on déduit $a \in I$.

Preuve de (2) : Si $J \in \mathcal{P}_{S^{-1}A}$, et si $x \in J$, alors $x = \frac{a}{s}$ avec $a = xs \in J \cap A$. L'inclusion $J \subset S^{-1}(J \cap A)$ est donc vraie. Réc., si $x \in S^{-1}(J \cap A)$, alors $x = \frac{a}{s}$ avec $a \in J \cap A$ et $s \in S$. Donc $a = xs \in J \cap A$, et cela entraîne $x \in J$ ou $s \in J$ (puisque J est premier). Comme $s \notin J$ (car $J \in \mathcal{P}_{S^{-1}A}$), on déduit $x \in J$. \square

4.a)

4) Si A ne possède qu'un seul idéal maximal M , alors bien sûr $M \subset A \setminus A^*$. Mais tout élément x de $A \setminus A^*$ est inclus dans un idéal maximal, donc ici $x \in M$. On a montré que $M = A \setminus A^*$ et que $A \setminus A^*$ était un idéal.

Réc. si $A \setminus A^*$ est un idéal et si M est un idéal maximal, M est inclus dans $A \setminus A^*$ (sinon $M \cap A^* \neq \emptyset \Rightarrow M = A$ absurde). La maximalité de M entraîne alors $M = A \setminus A^*$.

5.a)

$$5.b) \bullet \mathbb{Z}_t = \left\{ \frac{a}{t^n} \in \mathbb{Q} \mid a \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$$

$$\bullet \frac{a}{t^n} \in \mathbb{Z}_t^* \Leftrightarrow \exists b \in \mathbb{Z} \exists m \in \mathbb{N} \left(\frac{a}{t^n} \right) \left(\frac{b}{t^m} \right) = 1$$

$$\Leftrightarrow \exists b \in \mathbb{Z} \exists m \in \mathbb{N} \quad ab = t^{n+m}$$

$$\Leftrightarrow \exists \Delta \in \mathbb{N} \quad a = \pm t^\Delta$$

$$\text{mq } \boxed{\mathbb{Z}_t^* = \left\{ \pm t^k \mid k \in \mathbb{Z} \right\}}$$

• \mathbb{Z}_t est local : en effet $\mathbb{Z}_t \setminus \mathbb{Z}_t^*$ est un idéal - Bien le voir, il faut prouver l'implication

$$(*) \quad x = \frac{a}{t^n} \in \mathbb{Z}_t \setminus \mathbb{Z}_t^* \text{ et } \forall y = \frac{b}{t^m} \in \mathbb{Z}_t \Rightarrow xy \in \mathbb{Z}_t \setminus \mathbb{Z}_t^*$$

Par l'absurde : si l'on suppose $xy = \frac{ab}{t^{n+m}} \in \mathbb{Z}_t^*$, alors $ab = \pm t^\Delta$ ($\Delta \in \mathbb{N}$) donc, puisque t est premier, $b = \pm t^{\Delta'}$ ($\Delta' \in \mathbb{N}$). Cela entraîne $b \in \mathbb{Z}_t^*$ et c'est contraire à l'hypothèse. \square

• $\mathbb{Z}_5 = \left\{ \frac{a}{5^n} \in \mathbb{Q} \mid a \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$ et les idéaux premiers de \mathbb{Z}_5 s'écrivent $S_5^{-1}I$ où I est un idéal premier de \mathbb{Z} ne coupant pas S_5 . Donc $I = 0$ ou $I = (p)$ avec p premier et $p \neq 5$. Les idéaux premiers de \mathbb{Z}_5 sont :

$$(0), (2), (3), (7), (11), \dots,$$

5.c) Les idéaux premiers de \mathbb{Z}_{42}

seront : $(0), (5), (11), (13), \dots$ d'après la question 2).

6.a) La bijection est $I \mapsto S_t^{-1}I$ (donnée en 2))

et dire que $I \cap S_t = \emptyset$ équivaut à dire que $t \notin I$ (car I premier!)

6.b) On utilise un résultat connu : il y a bijection entre les idéaux premiers de $A/(t)$ et les idéaux premiers de A contenant (t) , et cette bijection est donnée par :

$$I \mapsto \pi(I)$$

où $\pi: A \rightarrow A/(t)$ est la projection canonique. La bijection réciproque est $J \mapsto \pi^{-1}(J)$.

6.c) Les idéaux premiers de $\mathbb{Z}/_{42}\mathbb{Z} = \mathbb{Z}/_{(42)}$ sont :

$$(0), (2), (3), (7)$$

7.a) (...)

7.b) A_I est local ?

$$\bullet A_I = \left\{ \frac{a}{s} \mid a \in A \text{ et } s \notin I \right\}$$

$$\bullet A_I^* = \left\{ \frac{a}{s} \mid a \notin I \text{ et } s \notin I \right\} \text{ . En effet :}$$

$$\frac{a}{s} \in A_I^* \Leftrightarrow \exists b \in A \exists s' \notin I \quad \frac{ab}{ss'} = 1$$

$$\Leftrightarrow \exists b \in A \exists s' \notin I \quad ab = ss' \notin I \quad (\text{cf } I \text{ premier})$$

$$\Rightarrow a \notin I.$$

Réc., si $a \notin I$ et $s \notin I$, alors $\frac{a}{s} \times \frac{s}{a} = 1$ donc $\frac{a}{s} \in A_I^*$.

• $A_I \setminus A_I^* = \{ \frac{a}{s} / a \in I \text{ et } s \notin I \}$ sera un idéal puisque :

$$\forall a \in I, \forall b \in A_I \quad \forall s, s' \notin I \quad \frac{a}{s} \cdot \frac{b}{s'} = \frac{ab}{ss'} \in A_I \setminus A_I^* \quad (\text{car } ab \in I).$$

Cela prouve que A_I est un anneau local..

7.c)

$$\mathbb{Z}_{(5)} = \left\{ \frac{a}{p_1^{a_1} \dots p_k^{a_k}} \in \mathbb{Q} / a \in \mathbb{Z} \text{ et } p_1, \dots, p_k \text{ premiers différents de } 5 \right. \\ \left. \begin{array}{l} a_1, \dots, a_k \in \mathbb{N} \\ k \in \mathbb{N}^* \end{array} \right\}$$

Les idéaux premiers de $\mathbb{Z}_{(5)}$ seront des $S_{(5)}^{-1} I$ où I est un idéal premier de \mathbb{Z} ne contenant pas $S_{(5)} = \mathbb{Z} \setminus (5)$, ie inclus dans (5) (d'après 2). Ce sera donc les idéaux :

$$\boxed{(0), (5)}.$$

Les idéaux premiers de $\mathbb{Z}/5\mathbb{Z}$ sont : $\boxed{(0) \text{ et } (5)}$ (cf 5.c).

FIN

Soit A un anneau non réduit à $\{0\}$, dont A et $\{0\}$ sont les seuls idéaux à gauche.

a) Montrer pour tout $a \in A$, la translation à droite $\delta_a: x \mapsto xa$ est soit nulle, soit bijective.

b) Supposons qu'il existe $a_0 \in A$ tq δ_{a_0} soit non nulle. Montrer l'existence d'un unique élément e de A tel que $ea_0 = a_0$. Prouver que $\forall x \in A$ $xe = x$ puis que $ex = x$ (on pourra considérer l'ensemble des éléments de la forme $x - ex$ pour démontrer ce dernier point)

c) En déduire que A est soit un anneau de corps nul (ie $\forall x, y \in A$ $xy = 0$) soit un corps.

a) (méthode: $\text{Im } \delta_a = \{xa / x \in A\}$ est un idéal à gauche de A puisque $0 = 0a \Rightarrow 0 \in \text{Im } \delta_a$, et:

$$\forall xa, ya \in \text{Im } \delta_a \quad xa - ya = (x - y)a \in \text{Im } \delta_a$$

$$\forall y \in A \quad \forall xa \in \text{Im } \delta_a \quad y \cdot xa = (yx)a \in \text{Im } \delta_a$$

Donc $\text{Im } \delta_a = \{0\}$ ou $\text{Im } \delta_a = A$, ie $\delta_a = 0$ ou δ_a surjective.

* Si $\delta_a \neq 0$, δ_a sera donc surjective. δ_a est un endomorphisme du groupe additif $(A, +)$, donc $\text{Ker } \delta_a$ est un sous-groupe de $(A, +)$. En fait, $\text{Ker } \delta_a = \{x / xa = 0\}$ est un idéal à gauche de A , donc $\text{Ker } \delta_a = \{0\}$ ou A . Comme $\delta_a \neq 0$, $\text{Ker } \delta_a \neq A$, donc $\text{Ker } \delta_a = \{0\}$ et δ_a sera injectif.

* Conclusion: $\delta_a = 0$ ou δ_a bijectif.

b) D'après la a), δ_{a_0} étant bijectif, il existera un et un seul élément e tel que $ea_0 = a_0$.
Par suite: $\forall x \in A$ $xe a_0 = xa_0$ ce qui entraîne $\boxed{xe = x}$ (puisque δ_{a_0} injectif).

* $\mathcal{I} = \{x - ex / x \in A\}$ est un idéal à gauche car:

1) $0 - e0 = 0 \in \mathcal{I}$

2) $(x - y) - e(x - y) = x - ex - (y - ey) \in \mathcal{I}$ dès que $x - ex$ et $y - ey \in \mathcal{I}$

3) $\forall y \in A \quad \forall x - ex \in \mathcal{I} \quad y(x - ex) = yx - \underbrace{yex}_y = yx - yx = 0 \in \mathcal{I}$

donc $\mathcal{I} = \{0\}$ ou A .

Si $\mathcal{I} = A$, il existerait $x_0 \in A$ tel que $x_0 - ex_0 = a_0 \Rightarrow e(x_0 - ex_0) = ea_0 \Rightarrow 0 = a_0$ absurde.

Donc $\mathcal{I} = \{0\}$ ie $\forall x \in A$ $x - ex = 0$

Cel: Si $\delta_{a_0} \neq 0$, A est un anneau unitaire, d'unité e .

c) Si $\exists x, y \in A$ $xy \neq 0$ alors $\exists a_0 \in A$ δ_{a_0} non nulle

On peut appliquer le b) : A sera un anneau unitaire, d'élément unité e .
 $A \neq \{0\}$ entraîne $e \neq 0$.

$\forall x \in A \setminus \{0\}$ $ex = x \neq 0$ donc δ_x n'est pas nulle, donc δ_x sera bijective (cf a)) et l'équation $yx = e$ admettra une unique solution x' .
 x' sera l'inverse à gauche de x ie $x'x = e$.

Montrons que x' sera aussi inverse à droite de x : pour cela, notons x'' l'inverse à gauche de x' . On a :

$$x''x' = e \quad \text{et} \quad x''x'x = x''e \Rightarrow ex = x'' \Leftrightarrow x = x''$$

donc bien $xx' = e$.

Cel : A sera un anneau unitaire dont tout élément non nul possède un inverse. Ce sera un corps.